REMARKS

In the aforementioned Office Action, claims 1-44 were examined. Claims 1-44 were rejected. In view of the following remarks, Applicants respectfully request reconsideration of the application.

Claim Rejection - 35 USC. §112

On page 5 of the Office Action, claim 36 stands rejected under 35 U.S.C. 112, first paragraph. The Examiner asserts, "because the specification, while being enabling for permitting access from any of the locations (Fig. 5F), does not reasonably provide enablement for 'wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers'." The Examiner questions "where control of the access is located, at the client or the server." The Examiner further asserts that the "disclosure does not disclose that the system controls the number of servers that a user gains access [to], instead the disclosure discloses the control of the location that the user can access from." Applicants respectfully traverse.

Applicants direct the Examiner's attention to paragraph 122, third sentence of the application describing an embodiment of the invention wherein a given requestor can only access secured items through at most one of said local servers at a time. "In one embodiment, instead of having three local modules, each permitting John to access from any of three locations, only one local module is configured to permit John to access form [sic] one of three locations at one time."

The Applicants further direct the Examiner's attention to paragraph 123 lines 2-6 of the application describing an embodiment including a dynamic configuration affecting access control management wherein the central server tracks users and permits access to secured documents from one local server at a time. The central server detects a user's location from the user's login at a local server. The server disables the user's access to any other local servers and enables the user's access to the local server where the user logs in. The dynamic configuration is illustrated in FIG. 5G as described below.

> "At one time, the system knows that John is accessing from location A. When John moves to location B, ***upon his login***, the central server (i.e., the user monitor in the server module) ***detects his whereabouts*** and thus notifies the local server manager 514 to reconfigure the local modules for both location A and location B. As shown in FIG. 5G, the local access control management 589 in a local server for location A is no longer responsible for John, while the local access control management 590 in a local server for location B takes over to be responsible for John. As a result, John is now permitted to access secured documents from location B but no longer from location A. FIG. 5H illustrates graphically that now John's accessibility has moved from location A to location B." (paragraph 123, lines 2-6, emphasis added)

Contrary to the Examiner's assertion, the specification does enable a person skilled in the art to make the invention commensurate with the scope of a "given requestor can only access secured items through at most one of said local servers at a time." Applicants respectfully submit that claim 36 is enabled by the specification.

Claim Rejections - 35 USC §102

On page 6 of the Office Action, claim 36 stands rejected under 35 U.S.C. 102(b) as being anticipated by Stallings (Cryptography and Network Security), hereinafter *Stallings*. The Examiner asserts that "Stallings teaches the Kerberos system comprising: a central server having a server module that provides overall access control (Kerberos authentication server page 333); and a plurality of local servers, each of said servers including a local module that provides local access control (last paragraph on page 333), wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (Kerberos authentication server Fig 11.2)."

The Examiner further asserts that *Stallings* teaches the Kerberos system "wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers (page 336 Session keys)." Applicants respectfully traverse.

Applicants are unable to identify a teaching of a "central server having a server module that provides overall access control" or a teaching of a "local module that provides local access control" in *Stallings*. *Stallings* teaches a realm or "a full-service Kerberos environment consisting of a Kerberos server, a number of clients, and a number of application servers." (*Stallings*, page 333, first full paragraph) "Such an environment is referred to as a realm." (*Stallings*, page 333, second full paragraph, first sentence)

Stallings further teaches a network of Kerberos realms wherein one Kerberos realm may provide service to another Kerberos realm. "[U]sers in one realm may need access to servers in other realms, and some servers may be willing to provide service to users from other realms." (*Stallings* page 333, last sentence)

If the examiner asserts that the "Kerberos server" is the "central server," then the examiner appears to contend that the "application servers" include the "local modules". However, if the application servers include the "local modules," then Applicants are unable to identify a teaching in *Stallings* of "a plurality of local servers, each of said servers including a local module that provides local access control." That is, there is no teaching in *Stallings* that each of the application servers includes a local module that provide local access control.

On the other hand, if the Kerberos server in a realm is the local server, then the Applicants are unable to identify "a central server having a server module that provides overall access control." The Examiner asserts that the authentication server provides overall access control. However, there is no teaching in *Stallings* that an authentication server in one realm provides access control for clients in another realm. Furthermore, there is no teaching in *Stallings* that an authentication server in realm A provides access control for servers in realm B to access secured items in realm C. Therefore, the authentication server in *Stallings* is not a central server having a server module that provides overall access control.

Moreover, there is no teaching in *Stallings* that a given requestor is permitted to access secure items **through** one or more of the said local servers. *Stallings* discloses that a requester that may access servers in more than one realm **from** one realm but not that a requestor may access secure items **through** one or more realms. "The user's client follows the usual procedures to gain access to the local TGS and then requests a ticket-granting ticket for a remote TGS (TGS in another realm). The client can then apply to the remote TGS for a service-granting ticket for the desired server in the realm of the remote TGS." (page 334, last two sentences)

Furthermore, there is no teaching in *Stallings* that "a given requestor, permitted to access secure items through one or more of said local servers, is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time." The Examiner argues that "(i)n order for serial access a new access ticket is required, just as in the parallel session, a new access is requested and therefore a new logon service and ticket and session key of the new access." However, there is no teaching in *Stallings* that using session keys "a given requestor, permitted to access secure items through one or more of said local servers, is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time." For example, a session key in realm A which controls access of a requestor through realm B would not prevent the same requestor from accessing secured items at the same time in realm D through a local server in realm E. The Applicants therefore assert that in *Stallings* a given requestor permitted to access secure items through one or more of said local servers, **is** able to access secured items through **more than one of said local servers at a time**. This is contrary to the limitations of claim 36 which recites in part that "a given requestor, permitted to access secure items through one or more of said local servers, is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through **at most one of said local servers at a time**" (emphasis added).

For at least these reasons, Applicants respectfully submit that *Stallings* does not anticipate claim 36. Because claims 37-44 depend directly or indirectly from claim 36 these claims are not anticipated for at least the same reasons as that of claim 36.

For example, Applicants are unable to find a teaching in *Stallings* of an "access control system as recited in claim 36, wherein said access control system couples to an enterprise network to restrict access to secured files stored therein." Applicants, therefore, request that the Examiner specifically point out an "access control system as recited in claim 36, wherein said access control system couples to an enterprise network to restrict access to secured files stored therein" or allow claim 37 and claims 38-44 which depend directly or indirectly therefrom.

Furthermore, the Examiner asserts that "(i)n reference to the local server having the ability to permit or deny access to requests to secured items by requestors, for example in the absence of the central server. The applicants have not claimed this feature." However, claims 39 and 40 do claim this feature. Claim 39 recites in part, "when the access requests are processed by said local servers, the requestors gain access to the secured files without having to access said central server." And, claim 40 recites in part, "the local module can be a copy of the server module so any of the local modules can operate independent of said central server and other of said local servers." Therefore, Applicants request that the Examiner allow claims 39 and 40 for at least the above reasons.

Claim Rejections - 35 USC §103

Claims 1-35

On page 7 of the Office Action, claims 1-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Samson et al (6,339,423), hereinafter *Samson* in view of Boebert et al (5,502,766), hereinafter *Boebert*. In reference to claims 1 and 34, the Examiner asserts that *Samson* discloses a system and method comprising all the elements of claims 1 and 34 except "authenticating the first client machine." The Examiner asserts that *Boebert* discloses the missing element in a system that "comprises an identification and authentication process for the user and the client machine (column 4, lines 26-35)." The Examiner asserts that "it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user," and "[o]ne of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only from terminals located inside the engineering area." Applicants respectfully traverse.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03.

As a motivation to combine *Samson* and *Boebert*, the Examiner states "(a)t the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as a system of *Boebert* in that authentication process of *Samson*. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form [sic] terminals located inside the engineering area." The Applicants traverse this statement. The Examiner suggests that the combination would be obvious because an advantage would be achieved. The Applicants respectfully point out that the requirements of a prima facie case under §103 include "some suggestion or motivation" for the combination, not that the combination would produce an advantage. An invention can be non-obvious while still producing an advantage.

The benefit must be apparent without the benefit of hindsight. It is, therefore, the position of the Applicants that the Examiner has not met the first element of a prima facie case for obviousness cited above. Specifically, the Examiner has not provided "some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings" as required to establish a prima facie case under §103.

Further, in contrast with the Examiner's suggested combination, *Samson* specifically teaches away from a data enclave and hardware in the form of a personal keying device resembling a calculator assigned to each user in a data enclave, as described in *Boebert*. For example, *Samson* teaches a system where a user authentication is stored in a "cookie" not a personal keying device. The cookie may be presented, by any of multiple client computers where a Multi-Domain Token Server may reside, upon request from Secondary Domain Agents for access to secured resources. "Upon receiving from Multi-Domain Token Server 208 a message confirming that the user has been authenticated, the Secondary Domain Agent transmits to the browser access control cookies that are associated with the domain of the Secondary Domain Agent." (*Samson*, lines 55-60, Col. 5)

In contrast, *Boebert* teaches a single domain in the form of a "data enclave" where "(d)ata can be restricted to a single organization" (lines 21-22, Col. 2) including a single server and a personal keying device assigned to each user in the enclave. "The present invention provides a data enclave for securing data carried on physical units of fixed and removable media in a network including a server and one or more workstations." (lines 39-42, Col. 5) The "identification and authentication process for the user and client machine" cited by the examiner in *Boebert* includes a piece of hardware resembling a calculator. "A personal keying device is assigned to each user in the enclave" (lines 47-48, Col. 5). The personal keying device resembles a calculator and can be restricted within the physical boundaries of the enclave.

> "Each user 5 is issued a Personal Keying Device 30. Personal Keying Devices 30 are used for key insertion and individual authentication. A Personal Keying Device 30 (shown in more detail in FIG. 6a) preferably contains fixed or removable electronic storage and processor 32, a keypad 34, a display 36, and a data transfer interface 38 that can be either wired or wireless (e.g., radio, infrared) and is compatible with an interface 31 on a Crypto Media Controller 26. The Personal Keying Device 30 can be highly portable, e.g., pocket calculator size. Personal Keying Devices 30 may also be equipped with theft detection circuitry to prevent them from being physically removed from the enclave working area." (*Boebert,* lines 34-47, Col. 9)

It is difficult to imagine the "Secondary Domain Agent" of *Samson* transmitting the calculator of *Boebert* to a browser.

Moreover, *Samson* teaches that there is a "major drawback" in controlling access to a set of servers that belong to only one domain.

> "A major drawback to a conventional access control system is that it only controls access to a set of servers and resources that belong to one domain. The underlying reason for this limitation is as follows. When a conventional access control system supplies access control cookies to a user that has just been authenticated, the cookies transmitted are associated with the domain of the access control system. When the browser requests access to another resource in another domain, the access control cookies are not transmitted because they are associated with the other domain. Thus, each domain name used to deploy a set of servers or resources requires its own implementation and maintenance of an access control system, adding to the expense of securing resources accessible over a network. In addition, for each domain name a user must login. Thus, the user may be encumbered by repetitious login procedures, or the number of domain names that may be used are limited by efforts to avoid encumbering the user." (*Samson,* lines 62-68, Col. 2 and lines 1-12, Col. 3)

> "Based on the foregoing, it is clearly desirable to provide an access control system that may be used to manage access to a set of resources deployed under multiple domain names, particular, requires a user to login just once to access the set of resources." (lines 13-17, Col. 3)

Thus, there is no motivation by a person of ordinary skill in the art implementing the system of *Samson* to restrict authentication of a user and to a keying device in a single domain. As such, there is no suggestion or motivation to combine *Sampson* with *Boebert*. Moreover, there must be some expectation of success. Applicants submit that the storing authentication information in the personal keying device of *Boebert* cannot be successfully combined with transmission of authentication information in cookies. Moreover, as discussed above, *Boebert* teaches confining the personal keying device within the physical boundaries of the enclave. Applicants respectfully submit that independent claims 1 and 34 are not obvious over *Samson* in view of *Boebert*. Because claims 2-20 depend from directly or indirectly claim 1, these claims are not obvious for at least the same reasons as that of claim 1.

Claims 21 and 35

In reference to claims 21 and 35, on page 8 of the Office Action, the Examiner applies the arguments set forth above for claims 1 and 34 to claims 21 and 35. Additionally, the Examiner asserts that *Boebert* discloses a system for "determining whether the user is permitted to gain access to secured items via the first location when said authenticating are successful."

As set forth above in regard to claims 1 and 34, Applicants respectfully submit that independent claims 21 and 35 are not obvious over *Samson* in view of *Boebert* because there is no motivation to combine Sampson with *Boebert, Samson* teaches away from *Boebert*, and there is no expectation of success.

Because claims 22-33 depend from directly or indirectly claim 21, these claims are not obvious for at least the same reasons as that of claim 21.

Conclusion

Based on the above remarks, Applicants believe that the rejections in the *Office Action* of July 14, 2006 are fully overcome, and that the application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicants' undersigned representative at the number given below.

Respectfully submitted,

Klimenty Vainstein et al.

Date: 9/14/2006

By: Ron Rohde

Ron Rohde, Reg. No. 45,050
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444